

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-008651

(43)Date of publication of application : 10.01.2003

(51)Int.Cl.

H04L 12/58

H04L 9/32

H04L 12/66

(21)Application number : 2001-188220

(71)Applicant : MITSUBISHI ELECTRIC CORP

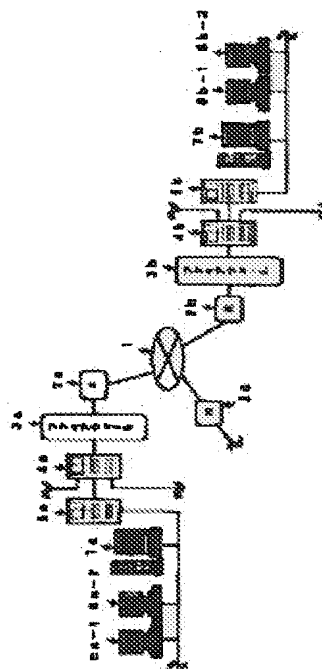
(22)Date of filing : 21.06.2001

(72)Inventor : UENO TOYOSHI

**(54) PACKET COMMUNICATION METHOD AND PACKET COMMUNICATION SYSTEM****(57)Abstract:**

**PROBLEM TO BE SOLVED:** To provide a packet communication method or the like which can oppose wire tapping and other tapping actions done over network lines and even high skillful tapping action done by being intruded into a receiver side server.

**SOLUTION:** The packet communication method sends and receives packetized communication data through a netted communication network, where the packet communication method extracts an authorized user ID corresponding to a local address, which is one of addresses showing a destination in a header added to the packets and which is an internal address of a local communication network that the destination belongs to, generates a temporary user ID different from the authorized user ID, generates a new header by inserting the temporary user ID into the header that the authorized user ID is extracted from, adds the new header to a data portion of the packet, composes a packet by inserting the extracted authorized user ID into the data portion, and sends the packet composed in the steps above mentioned to the destination.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-8651

(P2003-8651A)

(43) 公開日 平成15年1月10日 (2003.1.10)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テ-マ-ト* (参考)
H 0 4 L 12/58	1 0 0	H 0 4 L 12/58	1 0 0 C 5 J 1 0 4
9/32		12/66	B 5 K 0 3 0
12/66		9/00	6 7 3 A
			6 7 3 C

審査請求 未請求 請求項の数3 O L (全 8 頁)

(21) 出願番号 特願2001-188220 (P2001-188220)

(22) 出願日 平成13年6月21日 (2001.6.21)

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 上野 豊志

東京都千代田区丸の内二丁目2番3号 三  
菱電機株式会社内

(74) 代理人 100102439

弁理士 宮田 金雄 (外1名)

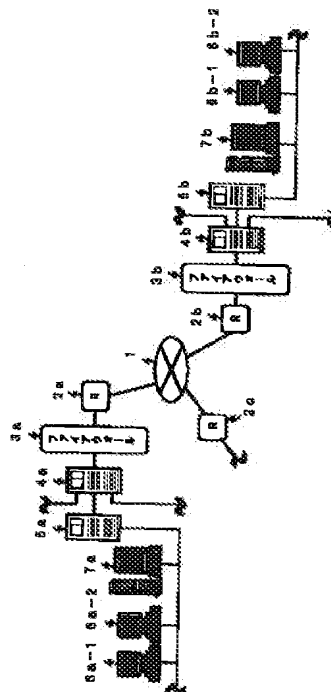
最終頁に続く

(54) 【発明の名称】 パケット通信方法及びパケット通信システム

(57) 【要約】

【課題】 タッピング等のネットワーク経路上において行われる盗聴行為、さらには受信側のサーバに侵入して行われる高度な盗聴行為に対しても有効に対抗し得るパケット通信方法等を提供する。

【解決手段】 網状の通信ネットワークを経由してパケット化された通信データを送受信するパケット通信方法において、上記パケットに付加されたヘッダ中の送信先を示すアドレスのうち、上記送信先が属するローカル通信ネットワークの内部アドレスであるローカルアドレスに対応する正規のユーザIDを抽出し、上記正規のユーザIDと異なる仮のユーザIDを発生し、この仮のユーザIDを上記正規のユーザIDが抽出されたヘッダ中に挿入して新規のヘッダを生成し、この新規のヘッダを上記パケットのデータ部分に付加すると共に、このデータ部分に上記抽出された正規のユーザIDを挿入してパケットを組み立て、上記工程により組み立てられたパケットを送信先に対して送信する。



## 【特許請求の範囲】

【請求項1】 網状の通信ネットワークを経由してパケット化された通信データを送受信するパケット通信方法において、上記パケットに付加されたヘッダ中の送信先を示すアドレスのうち、上記送信先が属するローカル通信ネットワークの内部アドレスであるローカルアドレスに対応する正規のユーザIDを抽出する工程と、上記正規のユーザIDと異なる任意のユーザIDを発生し、この任意のユーザIDを上記正規のユーザIDが抽出されたヘッダ中に挿入して新規のヘッダを生成する工程と、この新規のヘッダを上記パケットのデータ部分に付加すると共に、このデータ部分に上記抽出された正規のユーザIDを挿入してパケットを組み立てる工程と、上記工程により組み立てられたパケットを送信する工程とを備えたことを特徴とするパケット通信方法。

【請求項2】 上記送信パケットに暗号化処理又はスクランブル処理を施したことを特徴とする請求項1記載のパケット通信方法。

【請求項3】 網状の通信ネットワークに接続されたローカル通信ネットワーク内に設けられ、上記通信ネットワークに接続された他のローカル通信ネットワークとの間においてパケット化された通信データを送受信するサーバ装置と、このサーバ装置に接続され、上記サーバ装置に蓄積された自己宛の通信データの取り出し及び上記サーバ装置に対して生成した通信データの送信をそれぞれ行う複数の端末装置と、これら複数の端末装置からそれぞれ送信される通信データのパケットを編集し、そのパケットに付加された送信先の端末装置を示すアドレスのうちローカルアドレスに対応するユーザIDをパケット毎に書き替えて上記サーバ装置に出力し、かつ、上記サーバ装置から上記端末装置に取り出される通信データのパケットに付加されたローカルアドレスの識別を行い、自己が属するローカル通信ネットワークのローカルアドレス以外のローカルアドレスが付加されたパケットを蓄積し、蓄積した各パケットから正規のユーザIDを抽出したときは抽出した正規のユーザIDによりパケットを組み立て直して当該ユーザIDの端末装置に出力し、上記正規のユーザIDを抽出できなかったときは上記蓄積したパケットを破棄するパケット編集手段とを備えたことを特徴とするパケット通信システム。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 この発明は、インターネット等の通信ネットワークを利用して各種データの送受信を行うパケット通信システム及びパケット通信方法に関する。

## 【0002】

【従来の技術】 近年、コンピュータの普及やインターネット等の社会基盤の整備によりインターネット利用人口が拡大・増加しており、WWW（ワールド・ワイド・

ウェブ）、電子メール（E-mail）、IP（インターネット・プロトコル）電話等のインターネットを利用した各種のサービスが提供されている。

【0003】 このうち、電子メールサービスは、インターネットに接続されたメールサーバを介して相手との電子的なメッセージのやりとりを行うものであり、送信側から送信されたメッセージ（以下、送信メールという）は、相手（受信側）が不在の場合でも受信側のメールサーバに蓄積されており、あとで自由に読み出すことができるという特徴がある。ただし、不特定多数の者がアクセス可能なインターネット等の通信ネットワークを介して実現されるため、パケットフィルタリング等のいわゆる盗聴行為により送信メールの内容が他人に覗き見られるという問題があり、送信メールの暗号化やスクランブル等、盗聴行為を防止する各種の対策が行われている。

【0004】 例えば、特開2000-183967号公報には、送信パケットのヘッダ内のネットワークアドレス等を書き替えることにより、暗号化やスクランブル等の処理を用いることなくネットワーク経路上における盗聴行為による情報漏洩に対抗することができるパケット通信システムが記載されている。

## 【0005】

【発明が解決しようとする課題】 しかし、従来のパケット通信システムは、システムの構成上、各パケット通信装置毎に設定されるネットワークアドレスの数が制限されているため、例えば、相手先装置の近傍の1箇所においてタッピングによる盗聴行為が行われ、送信メールの全パケットが捕捉されてしまうと、ネットワークアドレスの同一性を解析されることにより、送信メールの内容が他人に知られてしまうという問題点があった。すなわち、インターネット等における電子メール等の盗聴は、タッピングポイントで収集したパケット群の中から目的のパケットのみを抽出し再組立によって通信内容を盗聴する方式がとられる。

【0006】 また、上述したような暗号化、スクランブル又はネットワークアドレスの書き替え等のいわゆる秘匿処理は、通常、受信側のメールサーバにおいて解除されてしまうため、たとえ送信時に暗号化、スクランブル及びネットワークアドレスの書き替え等の手段が施されていても、このような暗号化等が解除された後を狙った盗聴行為、例えば、受信側メールサーバの処理プログラムを書き替えて受信側のメールサーバに到着した送信メールの内容を盗聴する行為（例えば、目的の送信パケットに記述された送信先アドレスを書き替えて特定のアドレスに転送させるような処理を実行させる場合等）に対しては有効に対抗することができないという問題点があった。

【0007】 この発明は、上記のような課題を解消するためになされたもので、タッピング等のネットワーク経路上において行われる盗聴行為、さらには受信側のサー

パに侵入し、受信側サーバの処理プログラムを書き替えて受信側サーバに到着した特定の宛先の送信メール等を他のアドレスに転送させる等の高度な盗聴行為に対して有効に対抗することができる新規なパケット通信システム及びパケット通信方法を提供することを目的する。

【0008】

【課題を解決するための手段】請求項1の発明に係るパケット通信方法は、網状の通信ネットワークを経由してパケット化された通信データを送受信するパケット通信方法において、上記パケットに付加されたヘッダ中の送信先を示すアドレスのうち、上記送信先が属するローカル通信ネットワークの内部アドレスであるローカルアドレスに対応する正規のユーザIDを抽出する工程と、上記正規のユーザIDと異なる任意のユーザIDを発生し、この任意のユーザIDを上記正規のユーザIDが抽出されたヘッダ中に挿入して新規のヘッダを生成する工程と、この新規のヘッダを上記パケットのデータ部分に付加すると共に、このデータ部分に上記抽出された正規のユーザIDを挿入してパケットを組み立てる工程と、上記工程により組み立てられたパケットを送信する工程とを備えたものである。

【0009】請求項2の発明に係るパケット通信方法は、上記送信パケットに暗号化処理又はスクランブル処理を施したものである。

【0010】請求項3の発明に係るパケット通信方法は、網状の通信ネットワークに接続されたローカル通信ネットワーク内に設けられ、上記通信ネットワークに接続された他のローカル通信ネットワークとの間においてパケット化された通信データを送受信するサーバ装置と、このサーバ装置に接続され、上記サーバ装置に蓄積された自己宛の通信データの取り出し及び上記サーバ装置に対して生成した通信データの送信をそれぞれ行う複数の端末装置と、これら複数の端末装置からそれぞれ送信される通信データのパケットを編集し、そのパケットに付加された送信先の端末装置を示すアドレスのうちローカルアドレスに対応するユーザIDをパケット毎に書き替えて上記サーバ装置に出力し、かつ、上記サーバ装置から上記端末装置に取り出される通信データのパケットに付加されたローカルアドレスの識別を行い、自己が属するローカル通信ネットワークのローカルアドレス以外のローカルアドレスが付加されたパケットを蓄積し、蓄積した各パケットから正規のユーザIDを抽出したときは抽出した正規のユーザIDによりパケットを組立て直して当該ユーザIDの端末装置に出力し、上記正規のユーザIDを抽出できなかったときは上記蓄積したパケットを破棄するパケット編集手段とを備えたものである。

【0011】

【発明の実施の形態】実施の形態1. 以下、この発明の実施の形態1について図1乃至図3を用いて説明する。

図1はこの発明の実施の形態1によるパケット通信システムを示すシステム構成図であり、図1において、1は公衆通信網等の通信ネットワーク、2a、2b及び2cは通信ネットワーク1に接続されたルータ、3a、3bは各ルータ2a、2bに接続されたファイアウォール、4a、4bは各ファイアウォール3a、3bに接続された組織のメールサーバ、5a、5bは組織のメールサーバ4a、4bに接続された所属元のメールサーバ、6a-1、6a-2、6b-1、6b-2は所属元のメールサーバ5a、5bにそれぞれ接続された個人又は共通用の端末装置、7a、7bは所属元のメールサーバ5a、5bにそれぞれ接続され、後述するようなパケットの編集を行うパケット編集手段である。なお、メールサーバ4a、4b及び5a、5bはそれぞれ通信ネットワーク1上における電子郵便箱(mail box)に相当する機能を提供するサーバであり、いわゆる電子メールの送受信処理を実行する。また、ルータ2a、2b及び2cは通信ネットワーク1と各企業等に設けられたパケット通信システムとを接続するもので、これら各ルータ2a、2b及び2cのIPアドレスが各ローカル通信ネットワークの宛先として通信ネットワーク1上に公開されている。

【0012】次に動作についてさらに図2乃至図6を用いて説明する。図2は図1に示すパケット編集手段7a、7bの具体構成を示すブロック構成図、図3は図1に示すパケット通信システムの送信動作を説明するフローチャート図、図4は図1に示すパケット通信システムの送信動作を説明するフローチャート図である。なお、図1において、2a、3a、4a、5a、6a及び7aは送信側のパケット通信システム、2b、3b、4b、5b、6b及び7bは受信側のパケット通信システムを示し、それぞれ通信ネットワーク1に対してローカル通信ネットワークを構成しているものとする。また、この実施の形態では、送信側の端末装置6a-1から受信側の端末装置6b-2に対して電子メールの送信を行う場合を例として説明する。

【0013】例えば、送信側の端末装置6a-1において電子メールの作成が行われると、その電子メールはパケットと呼ばれる多数のデータに分割されて所属元のメールサーバ5aに対して送出される。この端末装置6a-1から送出されたパケット（以下、送信パケットという）は所属元のメールサーバ5aに出力される前にパケット編集手段7aに取り込まれて送信パケットの編集処理が行われる。図2に示すように、パケット編集手段7（送受信の区別をしない場合は単にパケット編集手段7という。他の構成も同様であり、送受信の区別をしない場合はa、bによる区別は行わない。）は送信処理部8及び受信処理部9をそれぞれ有しており、送信側のパケット通信システムにおける端末装置6a-1から創出された送信パケットは送信処理部8においてパケットの編

集処理が行われる。なお、受信側のパケット通信システムにおいて受信された電子メールは受信処理部9によりパケットの編集処理が行われるが、これについては後述する。以下、送信パケットの編集処理についてさらに図3を参照して詳細に説明する。

【0014】端末装置6a-1から送出された送信パケットは、先ず送信処理部8のパケット選択部10に取り込まれる(S01)。パケット選択部10に取り込まれた送信パケットはID抽出部11によりパケットの再組み立てに必要な固有データが抽出された後、データ変換部12に出力される(S02)。ここで、固有データとは、送信パケットのヘッダ中に挿入された送信先の端末装置の内部アドレスを示すローカルアドレスに対応したユーザIDである。各送信パケットのヘッダには送信先のアドレス、送信元のアドレス、パケット順序等を示す各種の情報が挿入されているが、そのうちの送信先の端末装置、例えば端末装置6b-1等の内部アドレスを示すローカルアドレスに対応したユーザIDが固有データとして抽出される。

【0015】図5は端末装置6a-1等において作成された電子メールのイメージ図であり、図5において、20はヘッダに挿入される情報部分、21はデータ部に分割される情報部分、22はヘッダ情報部20、データ情報部21の情報からなる電子メールである。図5に示すように、ヘッダ情報部20は送信元のアドレス、送信先のアドレス、送信日時、件名等の情報を有しており、これらの情報が分割された送信パケットの各ヘッダに挿入される。そして、各パケットのヘッダ中に挿入された送信先のアドレスのうち、送信先の端末装置の内部アドレスを示すローカルアドレスに対応したユーザID(図5に示す送信先を示すアドレスであるyyyy@yyy.yyy.co.jpのうち、yyyyの部分)の情報がID抽出部11により抽出される。なお、このような電子メール22の作成は各端末装置に設けられたメールソフト等を用いて作成することができる。

【0016】また、13はID抽出部11により抽出された正規のユーザIDに代わる任意のユーザIDを発生する変換データ発生部であり、この変換データ発生部13から出力されたヘッダ変換用のユーザIDがデータ変換部12に出力される(S03)。データ変換部12にはパケット選択部10において正規のユーザIDが抽出された後の各送信パケットが入力されており、変換データ発生部13から出力されたヘッダ変換用のユーザIDにより新規のヘッダが生成される(S04)。すなわち、端末装置6から送出された各送信パケットのヘッダが他のヘッダに変換されることになる。データ変換部12によりヘッダの変換が行われた送信パケットは、パケット組立部14に出力される。

【0017】パケット組立部14はデータ変換部13によりヘッダの変換が行われた送信パケットが入力される

と、その送信パケットのデータ部の任意の位置にID抽出部11により抽出された正規のユーザIDを挿入し、かつ、これらのデータが通信ネットワーク1の通信プロトコルに適合するようパケットの組立てを行って所属元のメールサーバ5aに出力する。例えば、インターネットの場合、トランスポート層のプロトコルに適合させるパケットの組立てが行われる(S05)。このように、パケット組立部14ではパケット選択部10に取り込まれた送信パケットとは異なる新たな送信パケットが組み立てられて所属元のメールサーバ5aに対して出力される(S06)。所属元のメールサーバ5aに送出された各送信パケットは組織のメールサーバ4aを経由して通信ネットワーク1にそれぞれ送出される。

【0018】通信ネットワーク1に送出された各送信パケットには送信先のメールサーバの外部アドレス(例えば、図5に示す送信先を示すアドレスであるyyyy@yyy.yyy.co.jpのうち、yyy.co.jpの部分)の情報が付与されており、通信ネットワーク1は各送信パケットに付与された送信先のメールサーバの外部アドレス、すなわちIPアドレスを参照しながら送信先の端末装置が属するメールサーバまで送信パケットを転送する。なお、図5に示す送信先を示すアドレスであるyyyy@yyy.yyy.co.jpのうち、@yyyの部分の部分は所属元のメールサーバのアドレス情報が付与された部分であり、この部分のアドレス情報により組織のメールサーバ4bから該当する所属元のメールサーバ5bに対して受信メールの転送が行われる。

【0019】このように、パケット編集手段7aはIPアドレスに該当する部分ではなく、ユーザIDの部分のデータを任意のデータに変換しているため、通信ネットワーク1に送出された送信パケットはヘッダ中に挿入された外部アドレスに従って送信先のメールサーバへ確実に送信される。なお、外部アドレスは変換していないので、送信先の端末装置6b-2が属する組織のメールサーバ4bのアドレスを対象としたパケットフィルタリング等により送信パケットを捕捉されるおそれがあるが、たとえ送信パケットが捕捉されても、内部アドレスであるユーザIDが他のユーザID、例えば、存在しないユーザIDに変換されており、また、各送信パケットの相関関係が破棄されており、どの端末装置を宛先とする送信パケットであるか識別することはできず、いわゆるパケットフィルタリングによる盗聴行為を防止することができる。

【0020】また、変換データ発生部13から出力されるヘッダ変換用のユーザIDの種類には制限がないので、全くランダムにユーザIDを発生させることで、変換データ発生部13から出力されるヘッダ変換用のユーザIDをランダム化することにより各送信パケット間の相関関係を破棄することができる。これによりパケットフィルタリングによる盗聴行為をさらに困難とするこ

とができ、仮に全ての送信パケットが捕捉され同一性の解析等がなされても、送信した電子メールの内容が他人に知られるおそれは極めて低い。

【0021】図6(a)は各端末装置6によりパケット化された送信パケットのデータ構成を示すデータ構成図、図6(b)はパケット組立部14において組み立てられた新たな送信パケットのデータ構成を示すデータ構成図である。図6(b)に示すように、パケット組立部14において組み立てられた新たな送信パケットには新規ヘッダ23bが付与されると共に、データ部24bに正規のユーザIDが挿入されている。このため、たとえ受信側メールサーバの処理プログラムを書き替えて受信側のメールサーバに到着した送信メールの内容を盗聴する行為、例えば、目的の送信パケットに記述された送信先アドレスを書き替えて特定のアドレスに転送させるような処理等がなされても、ヘッダ中に挿入された送信先の端末装置を示すユーザIDがランダム化されており、転送させる送信パケットの識別自体を行うことができず、このような盗聴行為に対しても有効に対抗することができる。なお、後述するように、受信側ネットワークのパケット編集手段7bでは、受信パケットを図6

(b)に示すパケット状態から図6(a)に示す状態に戻す編集処理が行われる。

【0022】次に受信動作について説明する。上述したとおり、送信側ネットワークのパケット編集手段7aを介して通信ネットワーク1に送出された送信パケットは、送信パケットのヘッダ中に挿入された送信先の外部アドレスが参照されて送信先である端末装置が属する受信側ネットワークのルータ2bに転送され、ファイアウォール3b、組織のメールサーバ4bを経由して所属元のメールサーバ5bに転送される。図5に示すようなメールアドレスは、通常、ローカル通信ネットワークの内部アドレスを示すユーザIDとその外部アドレスを示すDNS(domain name system)の部分で構成されており、DNSの部分は通信ネットワーク1内を転送される際に参照されるIPアドレスと関連付けられていることから変更することができないが、ユーザIDは通信ネットワーク1内における転送に関与しておらず、自由に変更することができる。

【0023】この実施の形態1によるパケット通信システムでは、送信パケットのヘッダ中に挿入された送信先のアドレスのうち、ユーザIDの部分のアドレス情報のみが編集され他の部分は正規のアドレス情報のままであるので、受信側ネットワークのルータ2bに到達した送信パケットはその送信先の端末装置が属する所属元のメールサーバ5bまで確実に転送することができる。

【0024】なお、パケット編集手段7bを設ける位置によって、パケット編集手段7におけるヘッダ変換の対象を変更することができ、組織のメールサーバ4bと所属元のメールサーバ5bとの間にパケット編集手段7を

設ける場合には、組織のメールサーバ4bまで受信パケットの転送が行われればよく、図5に示す送信先を示すアドレスであるyyyy@yyy.yyy.co.jpのうち、yyyy@yyyの部分のアドレス情報をパケット編集手段7におけるヘッダ変換の対象とすることができる。但し、ネットワークの上位にパケット編集手段7bを配置すると、その下位に接続されている全ての端末装置のパケット編集を負擔しなければならず、処理負擔を分散させる観点からネットワークの下位、例えば、所属元のメールサーバ毎、あるいは高度の盗聴防止機能が要求される端末装置群が属する所属元のメールサーバ5bのみを対象としてパケット編集手段7を配置することが望ましい。

【0025】所属元のメールサーバ5bに転送されたパケット(以下、受信パケットという)はヘッダ中に挿入されたユーザIDが他のユーザIDに変換されており、そのままではどの端末装置に対して送信されたパケットであるかを識別することができず、送信先の端末装置6b-2が所属元のメールサーバ5bに対してその受信メールの読出しを要求してもその受信パケットを送信先の端末装置6b-2に対して転送することはできない。そこで、所属元のメールサーバ5bに転送された受信パケットはパケット編集手段7bにより受信パケットの編集が行われる。上述したように、パケット編集手段7は送信処理部8及び受信処理部9をそれぞれ有しており、受信側ネットワークにおいて受信された受信パケットは受信処理部9において受信パケットの編集処理が行われる。以下、受信パケットの編集処理についてさらに図4を参照して詳細に説明する。

【0026】送信側のネットワークのパケット編集手段7aにおいてパケットの編集処理が行われた受信パケットは、まずパケット取得部15により取り込まれる(S07)。パケット取得部15により取得された受信パケットはパケット識別部16により対象とするパケットであるか否かが識別される(S08)。受信パケットのヘッダ中には送信先のアドレスが挿入されており、同一の送信先のパケットには同一のアドレスが挿入されているが、この実施の形態1によるパケット通信システムでは、送信パケットのヘッダ中に挿入された送信先のアドレス情報のうちユーザIDの部分のアドレス情報を他のユーザIDに変換しているため、対象となる受信パケットにおけるユーザIDはその受信側ネットワークには存在しないユーザID又は同一のユーザIDがないものとなっており、そのようなユーザIDを有する受信パケットは本発明に係るパケットの編集処理がなされた対象パケットであると判断して対象パケット蓄積部18に蓄積する(S09)。

【0027】また、通常、受信パケットは受信側のメールサーバ5bから各端末装置への転送において、MACアドレス(マシンアドレス)が参照されるが、送信側

の packets 編集手段7 a による packets の編集処理が行われた受信 packets はユーザ ID と MAC アドレスとが一致しないことから、エラーと認識され廃棄や送信元への返信等が行われる。しかし、この実施の形態による packets 通信システムでは、このようなエラーと認定される受信 packets のうち packets 編集手段7 b の送信処置部8において packets の編集処理が行われた packets を蓄積し受信 packets の再組立て処理を実行する。なお、packets 識別部16により対象 packets でないと判断された受信 packets は packets 編集手段7 による packets の編集処理がなされていないものと予想されるため、このような受信 packets については packets 破棄部17に出力され自動破棄される (S10)。

【0028】対象 packets 蓄積部18に蓄積された受信 packets は、正規のユーザ ID に基づく packets の再組立てを行うべく、packets 再組立部19に送られる。packets 再組立部19は、まず対象 packets 蓄積部17に蓄積された受信 packets のヘッダ中に挿入された送信先のアドレス情報のうち、ユーザ ID に関する情報を削除する。そして、その受信 packets のデータ部に挿入されている正規のユーザ ID を抽出し (S11)、この正規のユーザ ID を受信 packets のヘッダ中に挿入することにより受信 packets の再組立てを行う (S12)。packets 再組立部19は対象 packets 蓄積部18に蓄積された全ての受信 packets についてこのような packets の再組立てを行い、送信元の端末装置6 a-1 から送出された全ての送信 packets がこのような packets の再組立てにより元の packets 状態に戻され所属元のメールサーバ5 b に対して出力される (S13)。

【0029】このように、packets 再組立部19により組み立てられた受信 packets のヘッダ中には送信先の端末装置6 b-2 の内部アドレスを示す正規のユーザ ID が挿入されており、また、所属元のメールサーバ5 b は接続されている各端末装置6 b-1、6 b-2 等の内部アドレスを全て把握しているので、受信 packets がどの端末装置に対して送信された packets であるかを識別することができ、端末装置6 b-2 から受信メールの読出しの要求があった場合に送信側ネットワークの端末装置6 a-1 から送信された送信メールの内容を確実に送信先の端末装置6 b-2 に対して転送させることができる。

【0030】なお、この実施の形態1による packets 通信方法及び packets 通信システムにおいて、送信 packets の暗号化処理やスクランブル処理等を併用するように構成してもよい。この場合、さらにデータの保全効果を向上させることができる。また、この実施の形態1による packets 通信方法及び packets 通信システムは、電子メールデータの送受信を行うものであるが、データを packets 化して送受信する方式のものであれば、データの種類・内容に関係なく適用することが可能であり、メー

ルサーバのように受信した packets データを蓄積し端末装置から取り出すように構成された他のシステムにも適用することができる。

【0031】

【発明の効果】以上のように、請求項1に係る発明によれば、網状の通信ネットワークを経由して packets 化された通信データを送受信する packets 通信方法において、上記 packets に付加されたヘッダ中の送信先を示すアドレスのうち、上記送信先が属するローカル通信ネットワークの内部アドレスであるローカルアドレスに対応する正規のユーザ ID を抽出する工程と、上記正規のユーザ ID と異なる任意のユーザ ID を発生し、この任意のユーザ ID を上記正規のユーザ ID が抽出されたヘッダ中に挿入して新規のヘッダを生成する工程と、この新規のヘッダを上記 packets のデータ部分に付加すると共に、このデータ部分に上記抽出された正規のユーザ ID を挿入して packets を組み立てる工程と、上記工程により組み立てられた packets を送信する工程とを設けたので、タッピング等のネットワーク経路上において行われる盗聴行為、さらには受信側のサーバに侵入し、受信側サーバの処理プログラムを書き替えて受信側サーバに到着した特定の宛先の送信メール等を他のアドレスに転送させる等の高度な盗聴行為に対しても有効に対抗することができる。

【0032】また、暗号処理又はスクランブル処理を併用することにより、さらにデータの保全効果を向上させることができる。

【図面の簡単な説明】

【図1】 この発明の実施の形態1による packets 通信システムを示すシステム構成図である。

【図2】 図1に示す packets 編集手段7 a、7 b の具体構成を示すブロック構成図である。

【図3】 図1に示す packets 通信システムの送信動作を説明するフローチャート図である。

【図4】 図1に示す packets 通信システムの送受信動作を説明するフローチャート図である。

【図5】 端末装置6 a-1、6 b-1 等において作成された電子メールのイメージ図である。

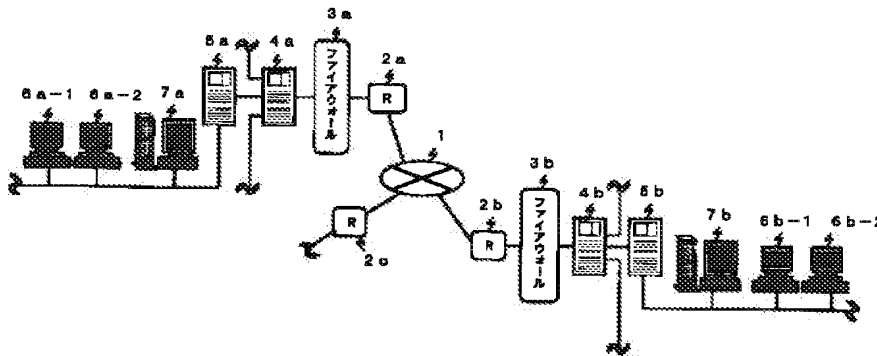
【図6】 図1に示す端末装置6 a-1 等により packets 化された送信 packets のデータ構成及び packets 編集手段7 a 等により packets の編集が行われた新たな packets のデータ構成を示すデータ構成図である。

【符号の説明】

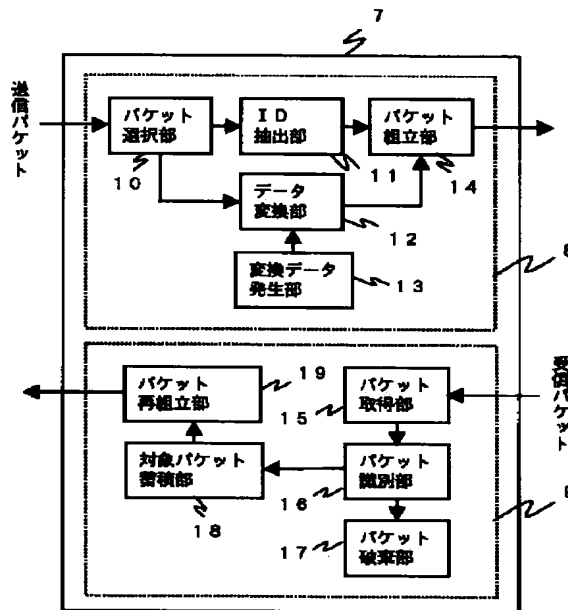
- 1 通信ネットワーク
- 2、2 a、2 b ルータ
- 3、3 a、3 b ファイアウォール
- 4、4 a、4 b サーバ装置 (組織のメールサーバ)
- 5、5 a、5 b サーバ装置 (所属元のメールサーバ)
- 6、6 a-1、6 a-2、6 b-1、6 b-2 端末装置

7, 7a, 7b パケット編集手段。

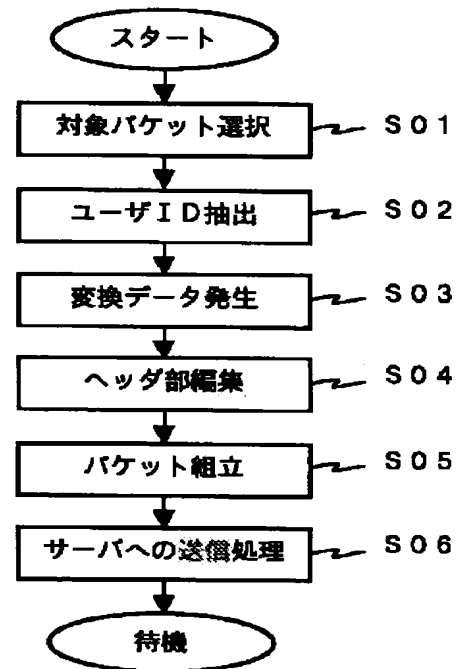
【図1】



【図2】

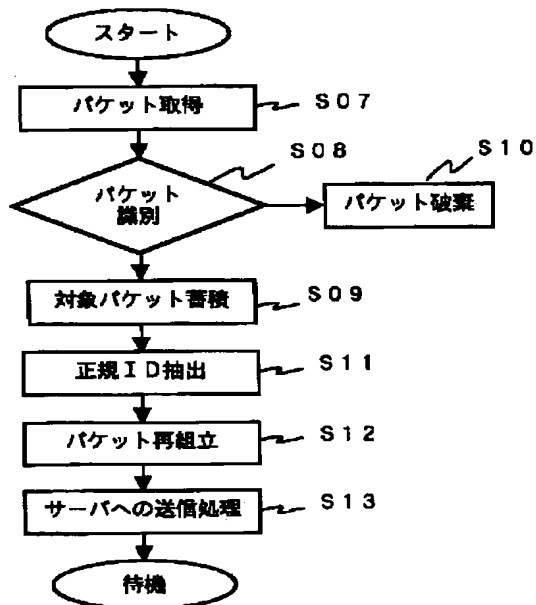


【図3】

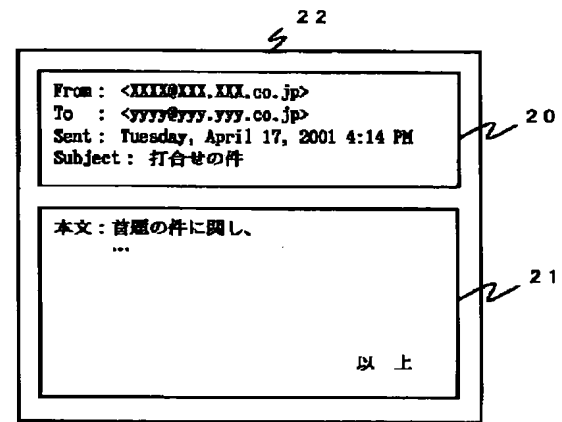




【図4】

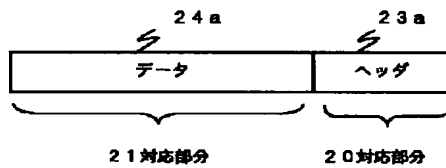


【図5】

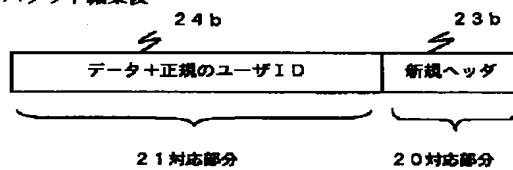


【図6】

(a) パケット編集前



(b) パケット編集後



フロントページの続き

Fターム(参考) 5J104 AA04 AA07 BA06 KA02 NA02  
 PA08  
 5K030 GA15 HA07 HB21 HC01 HC14  
 HD07 JA05 JA11 KA04 KA06  
 KX24 LB16 LC18 LD19 LE12  
 MB18